Cyber-Attack Penetration Test and Vulnerability Analysis

https://doi.org/10.3991/ijoe.v13i01.6407

Deris Stiawan
University Sriwijaya, Palembang, Indonesia
deris@unsri.ac.id

Mohd. Yazid Idris
Universiti Teknologi Malaysia
yazid@utm.my

Abdul Hanan Abdullah
Universiti Teknologi Malaysia
hanan@utm.my

Fahad Aljaber
Albaha University, Albaha, Saudi Arabia
fahadaljaber@hotmail.com

Rahmat Budiarto
Albaha University, Albaha, Saudi Arabia
rahmat@bu.edu.sa

Abstract—Hacking attempts or cyber-attacks to information systems have recently evolved to be sophisticated and deadly, resulting in such incidents as leakage of personal information and system destruction. While various security solutions to cope with these risks are being developed and deployed, it is still necessary to systematically consider the methods to enhance the existing security system and build more effective defense systems. Under this circumstance, it is necessary to identify the latest types of attacks attempted to the primary security system. This paper analyzes cyber attack techniques as well as the anatomy of penetration test in order to assist security officers to perform appropriate self security assesment on their network systems.

Keywords—Cyber Attack, Penetration Test, Security Audit.

1 Introduction

In the area of network security and cyber-attack hacking tools have been evolving, becoming easier to use, extremely comprehensive, readily available and easily accessible to the public. On the contrary, the technical capability to defend against attacks has tended towards decline in the face of these new threats. Therefore, it is necessary to test any proposed defense method against a penetration test in a live environment.

Penetration tests are useful measurement tools for discovering and addressing vulnerabilities in a network's infrastructure, showing just how vulnerable to malicious attack such networks truly are.

It is common for an attacker to exploit and to penetrate a victim's system without the owner's knowledge or consent. This exploit is sometimes achieved by implanting viruses or Trojan via the web or by sending malicious scripts in disguise via email, both of which provide easy ways for an attacker to infect their desired targets. As happened recently, Yahoo network has being hacked silently for two years and more that 5 millions customers information are being stolen. It may happened because of the lack of security awareness and regular security audit/ assessment.

In order to understand how to protect against as well as to prevent attacks, it is useful to understand from the attacker's perspective what methods they will use, what goals they have and how they launch their attacks. We believe that penetration test is a major element for all kinds of vulnerabilities and for evaluating overall systems. Furthermore, a little vulnerable information obtained should be of particular concern. The success of attacks is measured based on three factors: (i) complexity required to find vulnerability point in the systems, (ii) complexity to launch type of attack and (iii) complexity to detect the attack.

The rest of the paper is organized as follows. Section 2 presents related works which consists of two aspects: penetration test and network auditing analysis. Section 3 discusses the analysis of cyber attack techniques and penetration test, and finally Section 4 provides conclusions.

2 Related Works

The cyber-attack impacts describe by [1] intended to steal information by targeting specific resources to be stolen and disrupt their services. Then, [2] determine the anxiety and stress associated with possible internet hacking. Furthermore, a number of rationale and review of cyber war presented by [3] and [1].

An early analysis presented by [4] talked discusses the legalities, pros, and cons of conducting aggressive counter actions against cyber attackers. The study divideed hacking into three broad groups, those being damaging attempts, financially driven (fraud, black mail, and industrial espionage) and harmless browsing. Interestingly, hacking has become somewhat trendy. Meanwhile, [5] and [6] well define the taxonomies of the causes and costs of the attacks, and types of responses to the attacks.

In particular there are some various identified steps that attackers take when probing intent victim systems. These are commonly referred to as attack patterns, attack graphs or attack taxonomy depending upon the scenario in question. The definition of an attack graph by [7] and [8] are collection of scenarios that detail how a malicious agent can compromise the integrity of a targeted system. It represents prior knowledge about a given network in terms of vulnerabilities, exploits and connectivity. In contrast, work carried out by [9] represents an attack graph model as being based on a dependency relationships between vulnerabilities that enable certain exploits and existing security conditions.

Furthermore authors in [10] and [11], described four possible infiltration procedures as part of TCP/UDP and also authors in [12] presented characteristics of malicious threats that can be identified through source IP, destination IP, source port, destination port, and protocol used. Proposal work by [13], described how to discover potential

attack patterns launched against Microsoft's Windows Network environment as a target. They used a honeypot technique for capturing the habits of hackers attempting to gain access to their research system.

Meanwhile, there are four established dominant categories as widely used in the field of intrusion detection/prevention, seen previously in [14-18]. These categories are (i) Probes and scans to interrogate the active machine, gather information and find known vulnerabilities. (ii) Remote to Local (R2L) which attempts to send packets to the target over a network, then exploits the machine's vulnerabilities in order to illegally gain local access as a user without privileges. (iii) User to Root (U2R) for escalating privileges to gain access at a root level. (iv) Denial of Services (DoS) which is an unauthorized attempt to disrupt the normal functions and availability of a victim system, causing it to become too busy or too full to handle authorized requests from valid users.

3 Analysis of Attack Techniques and Penetration Test

3.1 Attack Techniques

An overview of common attack techniques is illustrated in Figure 1.

Label (a) represents the process of web implants, those being viruses and other forms of malware that can be attached to a web page with the intention of infecting users. Some hackers used entrapment techniques in which they entice users to click weblinks to land on pages that contain Trojans. At that point botnet controls are installed without notifying the end user, thus bypassing the regular procedures for executing code before ultimately starting a handshaking process with the intruder.

Label (b) represents viruses that are activated after opening an infected file from within an email attachment. In this case most users actively click on and execute the attached file, which then causes the Trojan program to get installed. From that point the attacker can use the Trojan as a backdoor through which they can gain access to the computer at the same privilege levels as the user who installed it.

In a more insidious form of attack, label (c) shows the process of SQL injections that attempt to find weaknesses on web pages or in backend systems. In this case the attacker is attempting to get database logins, database schemas, open the SQL console and interrogate what database version is running on the targeted machines. The aim of SQL injections are to discover the structures of databases, resulting in the attacker getting access to user privileges, leading to a web presence being defaced and possibly made into a threatening environment for its visitors.

Label (d) represents a web phising scenario, one in which an attacker uses carefully laid out steps in order to trick users into entering valid account details onto a web site that they think is valid, but that turns out to be a distinct URL setup specifically as a method for farming otherwise secure account details.

Label (e) is password guessing. This type of attack tends to be carried out by attempting passwords made up of words from a dictionary list one by one until a login is successful. For obvious reasons this form of attack is the most successful when the password in question was a simple word in the dictionary, however, brute force attacks make it possible for the application being used to try every possible combination of characters and strings of options.

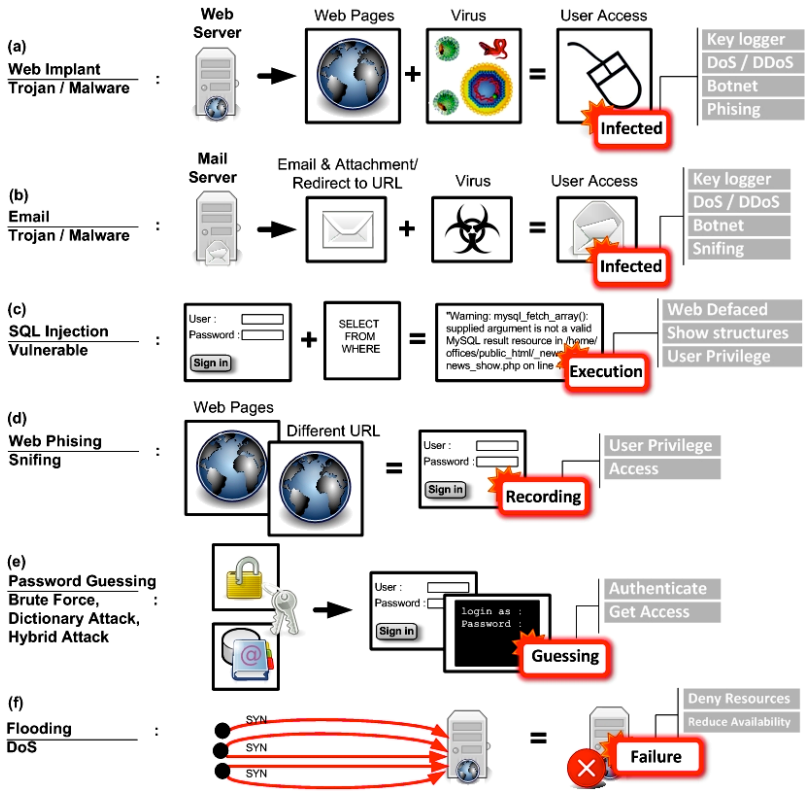

Fig. 1. Common variant of threats

Meaning that as computing power continues to grow, any standard deviation of normal words can ultimately fall before a brute force attack. That said, in this experiment it proved to be fairly ineffective due to the amount of time and resources needed to attack a wide variety of accounts, especially when the passwords consist of varying character and string combinations with more than six characters involved.

Label (f) shows flooding attacks, an attack type which involves sending many SYN packets without ACK to the target. This attack attempts to shut down a network by reducing bandwidth availability and increasing server load so as to deny the use of resources or services by authorized users.

3.2 Anatomy of Penetration Test

In 2011, authors in [6] began a discussion about the dark side of the Internet. In which damages come in the form of monetary loss, defamation, invasion of privacy and (in some cases) even physical harm. Furthermore, the loss of time and serious mental anguish can come as an extension of all of the above types of damages. Fortunately it is possible to protect against malicious forms of hacking.

Authors in [19] present characteristics of malicious threats that can be identified through source IP, destination IP, source port, destination port, and protocol used.

This study agrees with the position taken by [13] in that discovering a new attack pattern as soon as possible is a key part in maintaining an effective intrusion prevention system. Proposal by [19] was able to record forty-eight attack patterns whose information payload was based on attack patterns found using data held by the Common Attack Pattern Enumeration and Classification (CAPEC). Additionally, work performed by [20] described the top 10 vulnerable ports of widely-known services: port SSH (22), Micr. SQL (1433). RPC (135), SMB (445), 80 (Web), HTTPS (443). MySQL (3306), unknown/ possibility malware (8443, 12174, 6000).

According to researches presented by [6, 21-28], there are some steps and techniques commonly used when attempting to penetrate a system, those being:

1. Reconnaissance, which is a preparatory phase used to gather more information about the target.
2. Scanning, which is the pre-attack phase to find the basic information.
3. Gaining access, the first penetration phase, used to find holes in the system and get access to highly detailed information.
4. Maintaining access, in which the intruders establish control on an ownership level, leaving part of their presence in the system so as to gain at will access.
5. Clearing their tracks, in which the intruders hide traces of their activity by removing evidence from the system logs.

The methodology is used to gather information, scan for vulnerabilities and initiate penetration mechanisms (such as sniffing, password guessing, backdooring and flooding), as depicted in Figure 2.

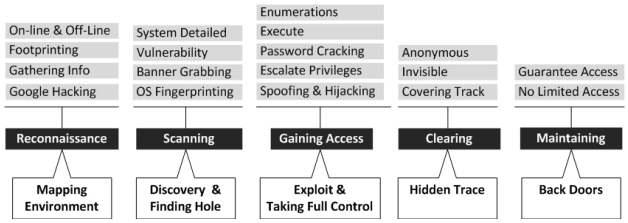

Fig. 2. Attack steps and technique

Gathering information includes finding some useful basic information, such as IP address, topology network, network resources and even personal information about the user which can be used in the next step. Search engines are typically used for obtaining information from online resources, while offline information gathering is achieved by bringing together scattered pieces of information coupled with social engineering to consolidate for a large amount of data that can be used for performing reconnaissance of a target environment. Social engineering is one of the easiest ways for an intruder to gain unauthorized access to a deliberately chosen target.

The next stage involves scanning and probing the target network in order to expose some vulnerabilities/security holes on the target machine. Actions that form up the majority of information probes include testing a system for response types, port scanning, active daemon and test the system by sending various queries to the target. Acknowledgement flow can be worked out by observing failure messages that come back to a system when a delivery problem has been detected. The aims of this stage are

to discover where the target is most vulnerable, such information can then be used in conjunction with the CERT Vulnerability Notes Database, CVE (Common Vulnerabilities and Exposures List), metasploit and the security community (CVE, Security Focus, National Vulnerability Database, Secunia, Microsoft Security Bulletin and Exploit search) in order to figure out the best way to gain access to the intended targeting machines.

From there, gaining access to an intended victim is achieved through direct penetration via password guessing, which includes trying to login to SSH, FTP, Telnet or HTTP connections using default installation access, combined with brute force password attempts. Determined attackers may also run packet sniffing for poisons, or attempt to observe the systems authentication process by capturing activity that occurs between the targeted machine and the client.

Once partial access is achieved, it is then common to implant malware, netbus and subseven to create a backdoor so as to grant full access. Installation of which usually occurs via a scarcely used network port so as to avoid notice. Backdoor access is very useful for maintaining access to the system without having to start from scratch, as well as for avoiding the recording log and security operators. The common backdoor used by attackers such as: netbus and subseven, which the attacker can use as a backdoor to gain access to the targeted machine with the same privileges as the user that unknowingly installed it. If successfully installed this kind of backdoor allows for the initialization of programs without the usual notifications being made to the hacked user. Some tools can also copy themselves on the machine, laying hidden until such a time as they are activated as part of a zombie attack intent on infecting further machines.

Finally, the most frustrating form of attack is achieved by launching a large number of packets at a target machine without acknowledging any particular port or protocol. This type of attack is known as a Denial of Service and is commonly used as a way to consuming all of the available service capacities of the target network. It achieves its goals by overloading the server, clogging up the network link, taking all the available memory resources and ultimately crashing the target server.

4 Conclusion

Penetration tests are useful measurement tools for discovering and addressing vulnerabilities in a network's infrastructure, showing how vulnerable to malicious attack such networks truly are. Thus, this study discussed the penetration test steps that were not revealed prior to attacks taking place. The knowledge on penetration test that elaborates how a cyber-attack happens is useful in providing guidelines for practitioners to protect their networks from any current potential cyber-attacks. It is important that security operators assume that they will be hacked and should e better to secure themselves for that reason.

With the aim of strenghtening the security of computer system, it is recommended to perform self security audit regularly. By knowing the hackers' way of thinking, a security officer is able to design an internal as well as external penetration test for the self security audit.

5 References

1. M. Morinaga, Y. Nomura, K. Furukawa, and S. Temma, "Cyber Attack Countermeasure Technologies Using Analysis of Communication and Logs in Internal Network," *FUJITSU SCIENTIFIC & TECHNICAL JOURNAL,* vol. 52, pp. 66-71, 2016.
2. J. D. Elhai and B. J. Hall, "Anxiety about internet hacking: Results from a community sample," *Computers in Human Behavior,* vol. 54, pp. 180-185, 1// 2016.
3. S. Zeadally and A. Flowers, "Cyberwar: The What, When, Why, and How [Commentary]," *IEEE Technology and Society Magazine,* vol. 33, pp. 14-21, 2014. https://doi.org/10.1109/MTS.2014.2345196
4. K. L. McLaughlin, "Cyber Attack! Is a Counter Attack Warranted?," *Information Security Journal: A Global Perspective,* vol. 20, pp. 58-64, 2011/02/11 2011.
5. V. Broucek and P. Turner, "Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective," *Journal of Computer Virology and Hacking Techniques,* vol. 9, pp. 27-33, 2013/02/01 2013.
6. W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and responses," *Information Systems,* vol. 36, pp. 675-705, 2011. https://doi.org/10.1016/j.is.2010.11.003
7. K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *Journal of Information Security and Applications,* vol. 29, pp. 27-56, 8// 2016.
8. J. Zhang, M. Zulkernine, and A. Haque, "Random-Forests-Based Network Intrusion," *MAN and Cybernetics,* vol. 38, pp. 649-659, 2008. https://doi.org/10.1109/TSMCC.2008.923876
9. L. Wang and S. Jajodia, "An Approach to Preventing , Correlating , and Predicting Multi-Step Network Attacks," ed: Springer, 2008, pp. 93-128.
10. A. Alhomoud, R. Munir, J. P. Disso, I. Awan, and A. Al-Dhelaan, "Performance Evaluation Study of Intrusion Detection Systems," *Procedia Computer Science,* vol. 5, pp. 173-180, 2011. https://doi.org/10.1016/j.procs.2011.07.024
11. J. M. Estévez-Tapiador, P. García-Teodoro, and J. E. Díaz-Verdejo, "Measuring normality in HTTP traffic for anomaly-based intrusion detection," *COMPUTER NETWORKS,* vol. 45, pp. 175-193, 2004. https://doi.org/10.1016/j.comnet.2003.12.016
12. G. Doss and G. Tejay, "Developing Insider Attack Detection Model : A Grounded Approach," 2009, pp. 107-112.
13. M.-y. Su, K.-c. Chang, and C.-y. Lin, "Attack Patterns Discovery by Frequent Episodes Mining from Honeypot Systems," ed: Springer, 2009, pp. 301-306. https://doi.org/10.1007/978-3-642-02617-1_31
14. S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *Computers & Security,* vol. 24, pp. 295-307, 2005. https://doi.org/10.1016/j.cose.2004.09.008
15. G. C. Tjhai, M. Papadaki, S. M. Furnell, and N. L. Clarke, "Investigating the problem of IDS false alarms: An experimental study using Snort," in *Proceedings of The Ifip, International Information Security Conference,* vol. 278, S. Jajodia, P. Samarati, and S. Cimato, Eds., ed: Springer Boston, 2008, pp. 253-267. https://doi.org/10.1007/978-0-387-09699-5_17
16. G. C. Tjhai, M. Papadaki, S. M. Furnell, and N. L. Clarke, "The Problem of False Alarms : Evaluation with Snort and DARPA 1999 Dataset," ed: Springer, 2008, pp. 139-150. https://doi.org/10.1007/978-3-540-85735-8_14
17. R. Beghdad, "Critical study of neural networks in detecting intrusions," *Computers & Security,* vol. 27, pp. 168-175, 2008. https://doi.org/10.1016/j.cose.2008.06.001

18. R. Beghdad, "Efficient deterministic method for detecting new U2R attacks," *Computer Communications,* vol. 32, pp. 1104-1110, 2009. https://doi.org/10.1016/j.comcom.2008.12.037
19. S. Barnum, "Attack Patterns: Knowing Your Enemy in Order to Defeat Them," ed: Cigital, 2007, pp. 1-51.
20. M. Molina, I. Paredes-Oliva, W. Routly, and P. Barlet-Ros, "Operational experiences with anomaly detection in backbone networks," *Computers & Security,* vol. 31, pp. 273-285, 2012. https://doi.org/10.1016/j.cose.2012.01.009
21. Barber Richard and A. Integralis, "Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated," *Computer Fraud & Security,* pp. 9-12, 2001.
22. S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers & Security,* vol. 24, pp. 31-43, 2005. https://doi.org/10.1016/j.cose.2004.06.011
23. Liu Zhijie, Wang Chongjun, and C. Shifu, "Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling," in *2008 International Conference on Information Security and Assurance*, 2008, pp. 214-219. https://doi.org/10.1109/ISA.2008.11
24. F. G. Marmol and G. M. Perez, "Security threats scenarios in trust and reputation models for distributed systems," *Computers & Security,* vol. 28, pp. 545-556, 2009. https://doi.org/10.1016/j.cose.2009.05.005
25. E. Claire, "Botnets: To what extent are they a threat to information security?," *Information Security Technical Report,* vol. 15, pp. 79-103, 2010. https://doi.org/10.1016/j.istr.2010.11.003
26. P. A. Raj Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," *Computer Communications,* vol. 34, pp. 1328-1341, 2011. https://doi.org/10.1016/j.comcom.2011.01.012
27. R. Sommer. (2012, Network Security Today: Finding Complex Attacks at 100Gb/s. *Informatik-Kolloquium, TU München,* 1-92. Available: http://www.icir.org/robin/slides/
28. A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security,* vol. 31, pp. 357-374, 2012. https://doi.org/10.1016/j.cose.2011.12.012

6 Authors

Deris Stiawan is with the Department of Computer Engineering, Faculty of Computer Science, University Sriwijaya, Palembang, Indonesia (deris@unsri.ac.id).

Mohd. Yazid Idris is with the Faculty of Computing, Universiti Teknologi Malaysia (yazid@utm.my).

Abdul Hanan Abdullah is with the Faculty of Computing, Universiti Teknologi Malaysia (hanan@utm.my).

Fahad Aljaber is with the College of Engineering, Albaha University, Albaha, Saudi Arabia (fahadaljaber@hotmail.com).

Rahmat Budiarto is with the Dept. of Computer Information System, College of Computer Science and Information Technology, Albaha University, Albaha, Saudi Arabia (rahmat@bu.edu.sa).

Submitted 09 November 2016. Published as resubmitted by the authors 16 December 2016.